

Spatially Correlated Qubit Errors and Burst-Correcting Quantum Codes

Farrokh Vatan, Vwani P. Roychowdhury and M. P. Anantram

Abstract— We explore the design of quantum error-correcting codes for cases where the decoherence events of qubits are correlated. In particular, we consider the case where only spatially contiguous qubits decohere, which is analogous to the case of burst errors in classical coding theory. We present several different efficient schemes for constructing families of such codes. For example, one can find one-dimensional quantum codes of length $n = 13$ and 15 that correct burst errors of width $b \leq 3$; as a comparison, a random-error correcting quantum code that corrects $t = 3$ errors must have length $n \geq 17$. In general, we show that it is possible to build quantum burst-correcting codes that have near optimal dimension. For example, we show that for any constant b , there exist b -burst-correcting quantum codes with length n , and dimension $k = n - \log n - O(1)$; as a comparison, the Hamming bound for the case with t (constant) random errors yields $k \leq n - t \log n + O(1)$.

Keywords— Quantum error-correcting code, Burst errors, Additive codes, Cyclic codes, Gilbert-Varshamov bound.

I. INTRODUCTION

THE theory of quantum error correction is now an active area of research [18], [5], [19], [20], [11], [2], [8]. Various techniques regarding construction of quantum error correcting codes based on classical codes have been proposed [18], [5], [19], [20], [8]. These papers typically assume the ‘independent qubit decoherence’ (IQD) model in which the decoherence of each qubit is uncorrelated to the decoherence of any other qubit as they all interact with separate reservoirs.

The IQD model is a valid assumption when the spatial separation of qubits in a quantum register is larger than the correlation length of the reservoir (or source of decoherence). Whether this condition is met or not will depend on specific physical models for quantum computers. The two main hardware proposals for quantum computers are the ion trap model [6] and the polymer chain model [12]. The exact nature of decoherence in these models is not well understood but we would expect the IQD model to break down in the polymer chain model where qubits are only a few Angstroms apart. Interaction with phonons whose spatial extent would be several atoms long will result in correlated decoherence of spatially continuous qubits. Reference [15] provided the first step in studying the effect of decoherence by assuming different models for interaction of qubits and the reservoir. Specifically, the effect of deco-

herence on a two-qubit system under circumstances when the IQD model is valid and when the correlation length of the reservoir is larger than the separation of the two qubits were studied. An important conclusion was that the second model for decoherence (i.e., where the correlation length is larger than the separation of qubits) leads to superdecoherence and subdecoherence of certain off diagonal elements of the density matrix in comparison to the IQD model.

If the details of the decoherence mechanism of qubits are known, then it might be possible to build more efficient error correcting codes compared to the IQD model. In classical error correction, it is well known that magnetic tapes used for storage are usually defective over length scales corresponding to a few bits. Then it is sufficient to code information on the tape so as to correct only spatially continuous errors. Similarly, in a classical communication channel, disturbances of the channel over short time periods lead to random single errors while disturbances over longer time periods lead to temporally continuous errors at the receiver. Such errors are called burst errors and the corresponding error correcting codes have significantly higher rates (see, e.g., [16]).

In this paper, we discuss a quantum analog of burst-error correcting codes. These codes would be important (i) when the coherence length of the reservoir is large enough to cause decoherence of spatially contiguous bits to be dominant, (ii) in storing of quantum information on a string of qubits (this case is similar to the magnetic tape case mentioned above; unintended impurities here may perturb the energy levels of a few contiguous qubits) and (iii) in communication of quantum information where entangled qubits would be temporally transported over an appropriate communication channel [2]. We show in this paper that when such correlated errors are dominant, then codes with higher rates than those obtained using the IQD model can be constructed.

The paper is organized as follows. In Section II, we present a review of quantum error-correcting codes. Here we present revised versions of known schemes for constructing quantum codes such that they can be applied for burst-error cases. In Section III, we give some results on binary cyclic codes, because these codes form the backbone of our constructions of quantum burst-correcting codes. In Section IV, we present some explicit constructions for quantum codes. In particular, we show how to construct quantum codes that map $k = n - 2 \log n - O(b)$ qubits to n qubits that corrects bursts of width b . In Section V, we first derive the Hamming and Gilbert-Varshamov type bounds for the maximum dimension of burst-correcting quantum codes. Then we show, for any constant b , there

F. Vatan is with the Electrical Engineering Department, UCLA, Los Angeles, CA 90095 (e-mail: vatan@ee.ucla.edu).

V. Roychowdhury is with the Electrical Engineering Department, UCLA, Los Angeles, CA 90095 (e-mail: vwani@ee.ucla.edu).

M. Anantram was with the Electrical Engineering Department, UCLA, Los Angeles, CA 90095. Present address: NASA Ames Research Center, M/S T27-A, Rm 104, Moffett Field, CA 94035-1000 (e-mail: anant@nas.nasa.gov)

exist b -burst-correcting quantum codes that have near optimal dimension; i.e., they map k qubits to n qubits where $k = n - \log n - O(1)$.

II. QUANTUM ERROR-CORRECTING CODES

In this section we provide basic definitions and notations about quantum error-correcting codes. We shall also describe various methods for constructing these codes; these techniques will be used in Section IV for constructing several different kinds of burst-correcting quantum codes.

A sequence of amplitude errors in qubits i_1, \dots, i_t of a block of n qubits can be represented by the unitary operator X_α , where the binary vector α of length n has 1 components only at positions i_1, \dots, i_t . Thus, for the basis $|v_1\rangle, \dots, |v_{2^n}\rangle$ of the 2^n -dimensional Hilbert space of n qubits, we have

$$X_\alpha |v_i\rangle = |v_i + \alpha\rangle. \quad (1)$$

Similarly, a sequence of phase errors can be written as

$$Z_\beta |v_i\rangle = (-1)^{v_i \cdot \beta} |v_i\rangle, \quad (2)$$

where the binary vector β represents the positions of errors, and $v_i \cdot \beta$ is the inner product of two binary vectors modulo 2. Note that

$$Z_\beta X_\alpha = (-1)^{\alpha \cdot \beta} X_\alpha Z_\beta. \quad (3)$$

Since we will be concerned with sets of errors with special structures, it is useful for us to consider a general setting, where a set \mathcal{E} of possible errors of the form $\pm X_\alpha Z_\beta$ is fixed (a similar approach is followed in [10]). Let $\bar{\mathcal{E}}$ be the set of the pairs (α, β) such that either $X_\alpha Z_\beta$ or $-X_\alpha Z_\beta$ is in \mathcal{E} . For example, the result of the entanglement of introducing at most t random errors in a state $|x\rangle$ can be represented as $\pm X_\alpha Z_\beta |x\rangle$, where $\text{wt}(\alpha \cup \beta) \leq t$ ¹. Therefore, in this case $\bar{\mathcal{E}} = \{(\alpha, \beta) \mid \text{wt}(\alpha \cup \beta) \leq t\}$. We will use the following notations:

$$\begin{aligned} \bar{\mathcal{E}}_X &= \{\alpha \in \{0, 1\}^n \mid (\alpha, \beta) \in \bar{\mathcal{E}} \text{ for some } \beta \in \{0, 1\}^n\} \cup \{\mathbf{0}\}, \\ \bar{\mathcal{E}}_Z &= \{\beta \in \{0, 1\}^n \mid (\alpha, \beta) \in \bar{\mathcal{E}} \text{ for some } \alpha \in \{0, 1\}^n\} \cup \{\mathbf{0}\}. \end{aligned}$$

For example, in the above example where \mathcal{E} is the set of at most t (random) errors, both $\bar{\mathcal{E}}_X$ and $\bar{\mathcal{E}}_Z$ are equal to $\{c \in \{0, 1\}^n \mid \text{wt}(c) \leq t\}$. The following result gives a necessary and sufficient condition for a set of quantum states to constitute a quantum code.

Theorem 1: ([2], [10]) A 2^k -dimensional subspace \mathcal{Q} of \mathbb{C}^{2^n} is an $((n, 2^k))$ error-correcting quantum code mapping k qubits to n qubits that protect against all errors in \mathcal{E} if

¹Here $\text{wt}(c)$ denotes the weight of the binary vector c , i.e. the number of 1-components of c ; and the binary vector $\alpha \cup \beta$ is the result of component-wise OR operation of α and β , for example $(011010) \cup (000110) = (011110)$.

for every orthonormal basis $|x_1\rangle, \dots, |x_{2^k}\rangle$ of \mathcal{Q} and every $e, e' \in \mathcal{E}$

$$\langle x_i | ee' | x_j \rangle = 0, \quad \text{if } i \neq j, \quad (4)$$

$$\langle x_i | ee' | x_i \rangle = \langle x_j | ee' | x_j \rangle. \quad (5)$$

If for all i , $\langle x_i | ee' | x_i \rangle = 0$, then the quantum code is said to be *non-degenerate*.

In [5], [19], [20] it is shown how to use classical error-correcting codes to build quantum codes. Although they stated their results when errors are (random) errors of weight at most t , their construction can easily be generalized for any set \mathcal{E} of errors. Before we state this result, we reiterate a definition concerning classical codes. Let \mathcal{C} be a subspace of $\{0, 1\}^n$, and \mathcal{F} be a subset of $\{0, 1\}^n$. We say \mathcal{C} has the ability to correct every error from \mathcal{F} (or simply, \mathcal{C} has \mathcal{F} -correcting ability) if and only if every two different elements e_1 and e_2 of \mathcal{F} belong to different cosets of \mathcal{C} ; or equivalently, $e_1 + e_2 \notin \mathcal{C}$.

Theorem 2: Let \mathcal{E} be a set of possible quantum errors. If there are $[n, k]$ classical codes \mathcal{C}_1 and \mathcal{C}_2 (with $2k > n$) such that $\mathcal{C}_2^\perp \subseteq \mathcal{C}_1$ and \mathcal{C}_1 has $\bar{\mathcal{E}}_X$ -correcting ability and \mathcal{C}_2 has $\bar{\mathcal{E}}_Z$ -correcting ability, then there is an $((n, 2^{2k-n}))$ quantum code that has \mathcal{E} -correcting ability.

Proof: Consider cosets of \mathcal{C}_2^\perp in \mathcal{C}_1 ; i.e., the sets of the form $a + \mathcal{C}_2^\perp$ with $a \in \mathcal{C}_1$. There are 2^{2k-n} different such cosets. Let $R = \{a_1, \dots, a_{2^{2k-n}}\}$ be the set of the representatives of distinct cosets. For the basis of the corresponding quantum code, we consider 2^{2k-n} vectors of the form $\sum_{c \in \mathcal{C}_2^\perp} |c + a\rangle$, where $a \in R$.

To check that the condition (4) holds, consider vectors

$$|x\rangle = \sum_{c \in \mathcal{C}_2^\perp} |c + a\rangle \quad \text{and} \quad |x'\rangle = \sum_{c \in \mathcal{C}_2^\perp} |c + a'\rangle.$$

(To simplify the notation, throughout this paper we delete the normalization factors.) If $a \neq a'$ then $\langle x | x' \rangle = 0$. Suppose $e = (-1)^\lambda X_\alpha Z_\beta$ and $e' = (-1)^{\lambda'} X_{\alpha'} Z_{\beta'}$ are in \mathcal{E} . Note that

$$\langle x | ee' | x' \rangle = \epsilon \langle x | Z_{\beta+\beta'} X_{\alpha+\alpha'} | x' \rangle, \quad (6)$$

for some $\epsilon \in \{-1, +1\}$. First suppose $\alpha + \alpha' \neq \mathbf{0}$. Then the right hand side of (6) is equal to

$$\epsilon \left\langle \sum_{c \in \mathcal{C}_2^\perp} |c + a\rangle \left| \sum_{c' \in \mathcal{C}_2^\perp} b_{c'} |c' + a' + \alpha + \alpha'\rangle \right. \right\rangle, \quad (7)$$

for some $b_{c'} \in \{-1, +1\}$. If $c + a = c' + a' + \alpha + \alpha'$, for some $c, c' \in \mathcal{C}_2^\perp$ and $a, a' \in \mathcal{C}_1$, then $\alpha + \alpha' \in \mathcal{C}_1$, which contradicts the $\bar{\mathcal{E}}_X$ -correcting ability of \mathcal{C}_1 . Therefore, $c + a \neq c' + a' + \alpha + \alpha'$, for every $c, c' \in \mathcal{C}_2^\perp$ and $a, a' \in \mathcal{C}_1$, thus inner product (7) is equal to zero. Now, suppose $\alpha + \alpha' = \mathbf{0}$. If $a \neq a'$ then then inner product (7) is obviously equal to zero. Finally, suppose $\alpha + \alpha' = \mathbf{0}$ and $a = a'$ (and of course $\beta \neq \beta'$), then the right hand side of (6) is equal to

$$\epsilon \sum_{c \in \mathcal{C}_2^\perp} (-1)^{(c+a) \cdot (\beta+\beta')} = \epsilon (-1)^{a \cdot (\beta+\beta')} \sum_{c \in \mathcal{C}_2^\perp} (-1)^{c \cdot (\beta+\beta')}.$$

Now the sum in the right hand side of the above equality is zero, because by $\bar{\mathcal{E}}_Z$ -correcting ability of \mathcal{C}_2 we have $\beta + \beta' \notin \mathcal{C}_2$. So the condition (5) holds. ■

Special case of the above theorem is when $\mathcal{C}_1 = \mathcal{C}_2$; thus we have the following corollary.

Corollary 1: Let \mathcal{E} be a set of possible quantum errors. If there is an $[n, k]$ classical code \mathcal{C} (with $2k > n$) such that \mathcal{C} is weakly self-dual (i.e., $\mathcal{C}^\perp \subseteq \mathcal{C}$) and \mathcal{C} has both $\bar{\mathcal{E}}_X$ -correcting ability and $\bar{\mathcal{E}}_Z$ -correcting ability, then there is an $((n, 2^{2k-n}))$ quantum code that has \mathcal{E} -correcting ability.

It is possible to generalize the above construction even for the case when \mathcal{C} is not weakly self-dual.

Theorem 3: Let \mathcal{E} be a set of possible quantum errors. Suppose there is an $[n, k]$ classical code \mathcal{C} such that \mathcal{C} has $\bar{\mathcal{E}}_X$ -correcting ability and \mathcal{C}^\perp has $\bar{\mathcal{E}}_Z$ -correcting ability. Let $\mathcal{D} = \{e + e' \mid e, e' \in \bar{\mathcal{E}}_X\}$. Then there is a quantum code that maps $n - k - \lceil \log_2 |\mathcal{D}| \rceil$ qubits to n qubits and has \mathcal{E} -correcting ability.

Proof: We shall prove this theorem by developing an algorithm to construct a quantum code. The basis of the quantum code consists of vectors of the form $|x_i\rangle = \sum_{c \in \mathcal{C}} |c + a_i\rangle$, for some binary vectors $a_i \in \{0, 1\}^n$. We shall show that one can choose $2^{n-k-\lceil \log_2 |\mathcal{D}| \rceil}$ such a_i 's for the quantum code.

Let $a_1 = \mathbf{0}$, so $|x_1\rangle = \sum_{c \in \mathcal{C}} |c\rangle$. Suppose $a_1, \dots, a_{\ell-1}$ have already been chosen. Then a_ℓ is any vector of $\{0, 1\}^n$ which is not of the form $c + a_i + \alpha + \alpha'$, for $c \in \mathcal{C}$, $1 \leq i \leq \ell-1$, and $\alpha, \alpha' \in \bar{\mathcal{E}}_X$. In this process it is possible to choose m vectors a_1, \dots, a_m if

$$m \cdot 2^k \cdot |\mathcal{D}| \leq 2^n.$$

The proof that conditions (4) and (5) hold is similar to the proof of Theorem 2. ■

In [3], [8] a general method for describing and constructing a special class of quantum error-correcting codes is proposed. Consider unitary operators $e_1 = X_{\alpha_1} Z_{\beta_1}, \dots, e_k = X_{\alpha_k} Z_{\beta_k}$, such that $e_i^2 = I$ (the identity operator) and $e_i e_j = e_j e_i$, for all i and j (i.e., $\alpha_i \cdot \beta_i = 0$ and $\alpha_i \cdot \beta_j + \alpha_j \cdot \beta_i = 0$, where the inner products are modulo 2). Consider the $k \times (2n)$ matrix

$$H = \left(\begin{array}{c|c} \alpha_1 & \beta_1 \\ \vdots & \vdots \\ \alpha_k & \beta_k \end{array} \right). \quad (8)$$

Suppose the matrix H has full rank over $\text{GF}(2)$. Then the set of the vectors $|x\rangle$ in \mathbb{C}^{2^n} such that $e_i |x\rangle = |x\rangle$, for all $1 \leq i \leq k$, form an $(n-k)$ -dimensional quantum code. The following theorem connects the error-correcting ability of this code with the properties of the dual space of H in $\{0, 1\}^{2n}$.

Theorem 4: ([3]) Let \mathcal{E} be a set of quantum errors. Suppose the $k \times (2n)$ matrix H in (8) is totally singular, i.e., $\alpha_i \cdot \beta_i = 0$ and $\alpha_i \cdot \beta_j + \alpha_j \cdot \beta_i = 0$ for all i and j . Let

\mathcal{C} denote the $[2n, k]$ binary code with H as its generator matrix. Then the space of the vectors $|x\rangle$ such that $X_{\alpha_i} Z_{\beta_i} |x\rangle = |x\rangle$, for all $1 \leq i \leq k$, is an $((n, 2^{n-k}))$ quantum code that has \mathcal{E} -correcting ability if for every $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in \bar{\mathcal{E}}$ either $(\alpha_1 + \alpha_2, \beta_1 + \beta_2) \in \mathcal{C}$ or $H \cdot (\beta_1 + \beta_2 \mid \alpha_1 + \alpha_2)^T \neq 0$.

III. RELEVANT RESULTS ON BINARY CYCLIC CODES

We construct different burst-correcting quantum codes (each with different dimensions) by utilizing Theorems 2, 3 and 4 when the underlying classical codes are cyclic. In this section we provide necessary facts and results concerning binary cyclic codes.

A linear subspace \mathcal{C} of $\{0, 1\}^n$ is called a *cyclic code* if \mathcal{C} is closed under the cyclic shift operator, i.e., whenever $(c_0, c_1, \dots, c_{n-1})$ is in \mathcal{C} then so is $(c_{n-1}, c_0, \dots, c_{n-2})$. When dealing with cyclic codes, it is much easier to identify each binary vector with a polynomial over the binary field $F_2 = \{0, 1\}$. For this, we represent every vector $c = (c_0, c_1, \dots, c_{n-1})$ in F_2^n by the corresponding polynomial $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$ in $F_2[x]$. For example, the vector $(1, 0, 0, 1, 1, 0)$ corresponds to the polynomial $1 + x^3 + x^4$.

One of the basic properties of a cyclic code \mathcal{C} is that \mathcal{C} can be generated by only one of its codewords. That is, there is a codeword in \mathcal{C} , represented by the polynomial $g(x)$, such that every codeword $c(x) \in \mathcal{C}$ is a multiple of $g(x)$, i.e., $c(x) = q(x) \cdot g(x)$ for some polynomial $q(x)$. Here the identity $c(x) = q(x) \cdot g(x)$ holds in the quotient ring $F_2[x]/(x^n + 1)$, i.e., we identify $q(x) \cdot g(x)$ with $q(x) \cdot g(x) \bmod (x^n + 1)$. It is well known that if the polynomial $g(x)$ generates the cyclic code \mathcal{C} of length n , then $g(x)$ is a factor of $x^n + 1$. (For more details see, e.g., [13].)

Some more useful notations: The *reciprocal* of a polynomial $f(x) = a_0 + a_1x + \dots + a_{m-1}x^{m-1} + a_mx^m$, with $a_m \neq 0$, is $f^*(x) = a_m + a_{m-1}x + \dots + a_1x^{m-1} + a_0x^m$, which is obtained from $f(x)$ by reversing the order of the coefficients. Note that $f^*(x) = x^m f(x^{-1})$. The *exponent* of the polynomial $f(x) \in F_2[x]$ is the least integer s such that $f(x)$ divides $x^s + 1$.

We start with stating some straight-forward facts about cyclic codes.

Lemma 1: Let \mathcal{C} be a cyclic code of length n generated by the polynomial $g(x) = 1 + \alpha_1x + \dots + \alpha_{k-1}x^{k-1} + x^k$ in $F_2[x]$.

(a) If $w(x) = x^j + a_1x^{j+1} + \dots + a_{\ell-1}x^{j+\ell-1} + x^{j+\ell}$ is in \mathcal{C} , then $\ell \geq k$.

(b) If $w \in \mathcal{C}$, $w \neq 0$ and w contains a block of m consecutive 0's, then $m < n - k$.

Proof: (a) Since $w(x) \in \mathcal{C}$ and \mathcal{C} is cyclic, the codeword represented by the polynomial $w'(x) = 1 + a_1x + \dots + a_{\ell-1}x^{\ell-1} + x^\ell$ should be in \mathcal{C} as well. This means

$$w'(x) = \sum_{i=0}^{n-k-1} \beta_i x^i g(x),$$

where $\beta_i \in \{0, 1\}$ are unique and at least one of β_i is nonzero (note that this equation holds in $F_2[x]$). The de-

gree of the right-hand side polynomial is at least k , so $\ell \geq k$.

(b) We can assume, w.l.o.g., that $w(x) = a_m x^m + \dots + a_{n-1} x^{n-1}$. Then $w(x) = \sum_{i=0}^{n-k-1} \alpha_i x^i g(x)$, for unique $\alpha_i \in \{0, 1\}$. It easily follows that $\alpha_0 = \dots = \alpha_{m-1} = 0$. The condition $w(x) \neq 0$ holds only if $m < n - k$. ■

In the next theorem we formulate a necessary condition for a cyclic code to be self-dual (in [9], this theorem has been derived in a slightly different form).

Theorem 5: Let a polynomial $g(x)$ of degree k ($k \leq n/2$) generate a cyclic code \mathcal{C} of length n . Let $g(x) = g_1(x) \cdots g_m(x)$ be a decomposition of $g(x)$ to irreducible polynomials. If the reciprocal of any of $g_i(x)$ is not among $g_1(x), \dots, g_m(x)$ (especially, none of the $g_i(x)$ is self-reciprocal), then \mathcal{C} is weakly self-dual, i.e., $\mathcal{C}^\perp \subseteq \mathcal{C}$.

Proof: Suppose $x^n + 1 = g(x)h(x)$. The cyclic code \mathcal{C}^\perp is generated by the polynomial $h^*(x) = x^{n-k} h(\frac{1}{x})$. Let $g^*(x)$ be the reciprocal of $g(x)$, i.e., $g^*(x) = x^k g(\frac{1}{x})$. Then

$$\begin{aligned} \mathcal{C}^\perp \subseteq \mathcal{C} & \text{ iff } h^*(x) \in \mathcal{C} \\ & \text{ iff } h^*(x) = p(x) \cdot g(x) \text{ for some } p(x) \\ & \text{ iff } x^{n-k} \cdot \frac{\frac{1}{x^n} + 1}{g(\frac{1}{x})} = p(x) \cdot g(x) \\ & \text{ iff } x^n + 1 = p(x) \cdot g(x) \cdot x^k g(\frac{1}{x}) \\ & \text{ iff } g(x) \cdot g^*(x) \text{ divides } x^n + 1. \end{aligned}$$

Let $g_i^*(x)$ be the reciprocal of $g_i(x)$. Then $g^*(x) = g_1^*(x) \cdots g_m^*(x)$. It is well-known (see, e.g., [13]) that if $g_i(x)$ is not self-reciprocal, then $g_i(x) \cdot g_i^*(x)$ divides $x^n + 1$. Therefore $g(x) \cdot g^*(x)$ divides $x^n + 1$ and \mathcal{C} is weakly self-dual. ■

Next we present a set of results on cyclic codes that correct burst errors. A *burst of width b* is a vector in $\{0, 1\}^n$ whose only nonzero components are among b successive components, the first and the last of which are nonzero. (The last component c_{n-1} of the vector $(c_0, c_1, \dots, c_{n-1})$ is understood to be adjacent to c_0 .) As mentioned in the previous section, we say a linear code \mathcal{C} has *burst-correcting ability b* if for all bursts w_1 and w_2 of width $\leq b$ we have $w_1 + w_2 \notin \mathcal{C}$. The following theorem gives a simple criterion for a cyclic code to have burst-correcting ability.

Theorem 6: Let \mathcal{C} be a cyclic code generated by the polynomial $g(x)$ of degree k . If $k \geq \frac{n}{2} + b$, then \mathcal{C} has burst-correcting ability b .

Proof: Suppose w_1 and w_2 are bursts of width $\leq b$. Then in $w_1 + w_2$ there is a block of at least $\frac{n}{2} - b$ consecutive 0's. Since $\frac{n}{2} - b \geq n - k$, by Lemma 1 (b), the theorem follows. ■

The following theorem by Fire [7] and Melas and Gorog [14] (see also [16]) gives a general method to construct interesting burst-correcting cyclic codes.

Theorem 7: Let $q(x)$ generate an $[n', k']$ code that has burst-correcting ability b . Let $p(x)$ be an irreducible polynomial of degree $\geq b$ and exponent e such that

$(p(x), q(x)) = 1$ (i.e., $p(x)$ and $q(x)$ have no common factor). Then the cyclic code \mathcal{C} of length $n = en'$ generated by $c(x) = q(x)p(x)$ has burst-correcting ability b .

In the following theorem we construct a small burst-correcting code. The interesting property of this code is that it is *weakly self-dual*; the property which is not addressed by the previous theorem.

Theorem 8: The polynomial $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^9$ generates a cyclic $[21, 12]$ code \mathcal{C} which has burst-correcting ability $b = 4$. Moreover, \mathcal{C} is weakly self-dual.

Proof: First note that $g(x)$ can be factored to irreducible polynomials as

$$g(x) = (1 + x + x^3)(1 + x^2 + x^4 + x^5 + x^6).$$

It is easy to see that the factors of $g(x)$ are factors of $x^{21} + 1$ (or look at the table of factors of $x^n + 1$ in [13]). So $g(x)$ generates a $[21, 12]$ cyclic code. From Theorem 5 it follows that \mathcal{C} is weakly self-dual.

It can be shown that \mathcal{C} has burst-correcting ability $b = 4$. ■

To utilize Theorem 7 for producing cyclic weakly self-dual codes that correct $b > 4$ bursts, we need to start with small cyclic weakly self-dual codes with burst-correcting ability b . It seems it is hard to find such codes with optimal, or near optimal, length. But it is possible to construct small cyclic weakly self-dual codes that correct *random* t errors. In the next lemma we give a construction for such codes. Although this approach does not lead to optimal codes, the result is enough to give rise to an infinite class of burst-correcting codes.

Lemma 2: For any t , there is a binary cyclic weakly self-dual $[n, k, 2t + 1]$ code with $n = 2^m - 1$ and $k = n - tm$, where $n > 2(2t - 1)^2$.

Proof: The desired code is a BCH code. We describe it by its cyclotomic cosets mod n (for details see [13]). The cyclotomic cosets which define the code are C_{2i-1} , for $1 \leq i \leq t$. Since $2t - 1 < \sqrt{n}$, all these cosets are distinct (see p.262 of [13]). So the code has minimum distance $2t + 1$. To prove the code is self-dual, we have to show for every i and j , $1 \leq i, j \leq t$, $n - (2j - 1) \notin C_{2i-1}$. If this is not true, then $n - (2j - 1) = (2i - 1)2^\ell$, for some integer ℓ . This implies that 2^ℓ should divide $2j$. But by assumption on n , we have $2^\ell > 2t$; which ends up in a contradiction. ■

IV. EXPLICIT CONSTRUCTION OF BURST-CORRECTING QUANTUM CODES

The *quantum burst-correcting codes* are defined naturally. Consider the set \mathcal{E} of quantum errors such that both $\overline{\mathcal{E}}_X$ and $\overline{\mathcal{E}}_Z$ are bursts of width $\leq b$. Then any quantum code that has \mathcal{E} -correcting ability is called a b -burst-correcting code.

First we show that there is a two-dimensional quantum code of length $n = 15$ that corrects burst errors of width $b = 3$. From the table given in [4], it follows that to correct $t = 3$ (random) errors one qubit should be mapped to at least 17 qubits.

We consider the cyclic $[15, 9]$ code \mathcal{C} generated by $1 + x^3 + x^4 + x^5 + x^6$. As it is noted in [16], this code corrects $b = 3$ burst errors. We show that the dual of this code has the same burst-correcting ability.

The dual code \mathcal{C}^\perp is generated by the polynomial $1 + x + x^4 + x^5 + x^6 + x^9$. So the following is a generator matrix for \mathcal{C}^\perp :

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

We want to show that if b_1 and b_2 are two bursts of width ≤ 3 and $b_1 \neq b_2$, then $b_1 + b_2 \notin \mathcal{C}^\perp$. First note that $b_1 + b_2$ contains a block of at least 5 consecutive 0's. Then w.l.o.g. we can assume $b_1 + b_2 = (00000 \star \star \dots \star)$ or $b_1 + b_2 = (000001 \star \star \dots \star)$. If $b_1 + b_2 \in \mathcal{C}^\perp$, then in the first case we would have $b_1 + b_2 = 0$, i.e., $b_1 = b_2$ which contradicts the assumption $b_1 \neq b_2$; and in the second case $b_1 + b_2 = (000001100111001)$ which is not sum of two bursts of width ≤ 3 . This completes the proof that \mathcal{C}^\perp corrects bursts of width 3.

Now we show that the all-one vector $\mathbf{1}$ is not in the coset of any vector of the form $b_1 + b_2$, where b_1 and b_2 are bursts of width ≤ 3 . Assume, by contradiction, that $\mathbf{1} + b_1 + b_2 \in \mathcal{C}^\perp$. Since $b_1 + b_2$ has a block of at least 5 consecutive 0's, $\mathbf{1} + b_1 + b_2$ is either $(111110 \star \star \dots \star)$ or $(111111 \star \star \dots \star)$. In the first case $\mathbf{1} + b_1 + b_2$ is (111110111010001) and in the second case it is (111111011101000) . So $b_1 + b_2$ is either (000001000101110) or (000000100010111) ; which in neither case it can be the sum of two bursts of width ≤ 3 .

So a basis for the desired quantum code consists of $|0_L\rangle = \sum_{c \in \mathcal{C}} |c\rangle$ and $|1_L\rangle = \sum_{c \in \mathcal{C}} |c + \mathbf{1}\rangle$.

Eric Rains [17] has brought to our attention that there is a 3-burst-correcting quantum code with smaller length. This is a $[[13, 1, 5]]$ code. The stabilizer of this code is defined by a quadratic residue code over $\text{GF}(4) = \{0, 1, \omega, \bar{\omega} = \omega^2\}$ with $g(x) = (1 + x)g_1(x)$ as its generator polynomial, where $g_1(x) = 1 + \bar{\omega}x + \omega x^3 + \bar{\omega}x^5 + x^6$ (see [4] for details on quantum codes defined by codes over $\text{GF}(4)$). Here it is enough to show that the cyclic code \mathcal{C} (over $\text{GF}(4)$) generated by the polynomial $g_1(x)$ is a 3-burst-correcting code. Suppose the nonzero polynomial $q(x)$ (of degree ≤ 12) represents a codeword in \mathcal{C} that is a sum of two bursts of width ≤ 3 . Then at least 7 coefficients of $q(x)$ are zero. Therefore, without loss of generality, we can assume $q(x) = 1 + a_1x + \dots + a_8x^8$. Hence $q(x) = (1 + ax + bx^2)g_1(x)$, for some $a, b \in \text{GF}(4)$. But for any a and b the corresponding $q(x)$ is not a sum of two bursts of width ≤ 3 .

Now we show the existence of infinite classes of quantum burst-correcting codes.

Theorem 9: If there is a binary $[n, k]$ code \mathcal{C} (with $k < \frac{n}{2}$) such that \mathcal{C} and \mathcal{C}^\perp both have burst-correcting ability b ,

then there is an $((n, 2^K))$ quantum code with $K = n - k - 2\lceil \log n \rceil - b$ that corrects all burst errors of width b .

Proof: It follows from the fact that the number of vectors of the form $w_1 + w_2$, where w_1 and w_2 are bursts of width $\leq b$, is at most $n^2 \cdot 2^b$ and the Theorem 3. ■

Corollary 2: There are $((n, 2^k))$ quantum codes with $n = (2^m - 1)(2b - 1)$ and $k = n - m - 2\lceil \log n \rceil - 3b + 1$ having burst-correcting ability b .

Proof: From Theorem 7 with $n' = 2b - 1$, $q(x) = x^{2b-1} - 1$ and $p(x)$ any primitive polynomial of degree m such that $m > 2b - 1$, we get an $[n, n - m - 2b + 1]$ binary code \mathcal{C} having burst-correcting ability b . If $m \geq 3$, then we can apply Theorem 6 to show that \mathcal{C}^\perp also has burst-correcting ability b . Then the result follows by applying Theorem 9. ■

For any fixed constant b , the above result gives a family of quantum codes of length n and dimension $n - 3\log n - O(1)$ having burst-correcting ability b . In the next theorem we show that for $b \leq 4$ we can construct burst-correcting quantum codes with dimension $n - 2\log n - O(1)$.

Theorem 10: For every $m \geq 7$, there is an $((n, 2^k))$ quantum code with $n = 21(2^m - 1)$ and $k = n - 2m - 18$ having burst-correcting ability $b = 4$.

Proof: We utilize Theorem 7 for $q(x)$ the degree 9 polynomial given in Theorem 8 and $p(x)$ any primitive polynomial of degree ≥ 7 . Since $p(x)$ is primitive, it is not self-reciprocal. Thus we obtain a binary $[n = 21(2^m - 1), k = n - m - 9]$ code \mathcal{C} , which is weakly self-dual by Theorem 5. Now by applying Corollary 1, we get the quantum code with the given parameters. ■

By utilizing Lemma 2, we can get a similar result for the case $b > 4$. The following theorem shows how to construct $((n, 2^K))$ quantum codes, with $K = n - 2\log n - O(1)$, for constant burst-width b .

Theorem 11: For every b , there is an $((n, 2^k))$ quantum b -burst-correcting code, where $n = (2^{m'} - 1)(2^m - 1)$, $k = n - 2m - 2bm'$, $2^{m'} > 2(2b - 1)^2$ and $m > m'$.

Proof: As in the previous theorem, we utilize Theorem 7, where $q(x)$ is the generator polynomial of the BCH code of length $n' = 2^{m'} - 1$ given in Lemma 2, and $p(x)$ is any primitive polynomial of degree $m > m'$. ■

V. BOUNDS AND A NEW SCHEME FOR CONSTRUCTION

In this section, we present general upper and lower bounds for maximum dimension of a quantum burst-correcting code.

Theorem 12: Let \mathcal{E} be a set of errors, and $\mathcal{D} = \{e + e' | e, e' \in \mathcal{E}\}$. Let 2^k be the maximum dimension of any non-degenerate quantum code of length n that has \mathcal{E} -correcting ability. Then

$$n - \log_2 |\mathcal{D}| \leq k \leq n - \log_2 |\mathcal{E}|.$$

Proof: Let $|x_1\rangle, \dots, |x_{2^k}\rangle$ be a basis for a quantum code of dimension 2^k . The upper bound (*The Hamming bound*) follows from this fact that, by (4), in the space \mathbb{C}^{2^n}

the $2^k|\mathcal{E}|$ vectors of the form $X_\alpha Z_\beta |x_i\rangle$ should be orthogonal, and hence independent.

The lower bound (*The Gilbert–Varshamov bound*) follows from an argument similar to the one given in [3]. ■

Corollary 3: Let 2^k be the maximum dimension of any non-degenerate quantum code of length n which has burst-correcting ability b . Then

$$n - 2 \log_2 n - 2b \leq k \leq n - \log_2(n - b + 2) - 2b - 3.$$

Proof: It is enough to note that in this case $|\mathcal{E}| = 3 \cdot 4^{b-1}(n - b + 4/3)$, and $|\mathcal{D}| \leq 4^b n^2$. ■

Next we present a new scheme for constructing quantum codes from classical linear codes. By utilizing this method, for fixed constant b , we obtain b -bursts-correcting quantum codes of length n with dimension $n - \log_2 n - O(1)$. These are almost optimal codes (compare with the bound given in Corollary 3).

Theorem 13: If there is a $(3b)$ -burst correcting binary $[n, k]$ cyclic code \mathcal{C} such that \mathcal{C} is weakly self-dual, then there is a (non-degenerate) b -burst-correcting $((n, 2^k))$ quantum code.

Proof: Suppose the $(n - k) \times n$ matrix H is a parity check matrix for \mathcal{C} . Let $H^{\rightarrow m}$ denote the matrix that is obtained from H by shifting (cyclically) the columns m times to the right. Note that $H^{\rightarrow m}$ is also a parity check matrix of \mathcal{C} , because \mathcal{C} is cyclic. Now, consider the stabilizer defined by the matrix

$$G = [H + H^{\rightarrow b} \mid H + H^{\rightarrow 2b}].$$

It is easy to check that G is indeed a totally singular matrix. Suppose $e = (e_1 \mid e_2)$ and $e' = (e'_1 \mid e'_2)$ are bursts of width $\leq b$, and $e \neq e'$. Let

$$w = e_1 + e'_1 + (e_1 + e'_1)^{\leftarrow b} + e_2 + e'_2 + (e_2 + e'_2)^{\leftarrow 2b},$$

where $e^{\leftarrow m}$ denotes the vector obtained by cyclically shifting e to the left m times. Then it is easy to check that $w \neq 0$ and w is the sum of two bursts of width $\leq 3b$. So $w \notin \mathcal{C}$ and

$$G \cdot (e + e')^T = H \cdot w^T \neq 0.$$

Now the theorem follows from Theorem 4. ■

To apply the above theorem, we need weakly self-dual b -burst-correcting binary codes with arbitrary length. For $b \leq 4$, Theorem 8 gives explicit construction of such codes. In general, we can apply the following theorem.

Theorem 14: ([1]) For every b and for every square-free polynomial $e(x)$ of degree $b - 1$ and of index m_e such that $e(0) \neq 0$ and for every sufficiently large $m \equiv 0 \pmod{m_e}$, a primitive polynomial $p(x)$ of degree m exists such that $e(x)p(x)$ generates a b -burst-correcting code of length $n = 2^m - 1$ and dimension $k = n - m - b$.

To get weakly self-dual codes, choose $e(x)$ to be any primitive polynomial of degree $b - 1$. Then $e(x)p(x)$ generates a weakly self-dual b -burst-correcting code, because

no primitive polynomial is self-reciprocal. Thus we get the following bound for burst-correcting quantum codes.

Theorem 15: For every b and for sufficiently large $n = 2^m - 1$ (where $m \equiv 0 \pmod{m_b}$ for some fixed integer m_b depending only on b), there are (non-degenerate) b -burst-correcting quantum codes of length n and dimension $n - m - 3b$.

VI. CONCLUDING REMARKS

We described different schemes for constructing quantum burst-correcting codes. As expected, these classes of codes are more efficient than codes that protect against random errors. More specifically, to protect against burst errors of width b (where b is a fixed *constant*), it is enough to map $n - \log n - O(1)$ qubits to n qubits, while in the case of t random errors (for *constant* t) at most $n - t \log n + O(1)$ qubits can be mapped to n qubits (the best construction so far maps $n - (t + 1) \log n - O(1)$ qubits to n qubits, for $t = 2$ and 3, see [4]).

We present an explicit construction of almost optimal quantum code for bursts of width ≤ 4 . It would be interesting to find similar explicit constructions for bursts of larger width. Also, our constructions work for specific values of n , the length of the quantum code. It remains open how to generalize these constructions for other values of n . Finally, in Theorem 13 we develop a novel method to obtain quantum codes from binary codes such that the rate of the quantum code (for a constant number of errors) has the same order of magnitude as the binary code. If this method can be generalized to other classes of quantum codes, there might be a significant improvement in the rate of the existing quantum codes.

ACKNOWLEDGEMENTS

We would like to thank Eric Rains for helpful comments and the example of $[[13, 1]]$ 3-burst-correcting code. We are also grateful to the referees for useful comments and suggestions.

REFERENCES

- [1] K. A. S. Abdel-Ghaffar, R. J. McEliece, A. M. Odlyzko, and H. C. A. van Tilborg. On the existence of optimum cyclic burst-correcting codes. *IEEE Trans. Information Theory*, IT-32(6):768–775, 1986.
- [2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed state entanglement and quantum error correction. *Phys. Rev. A*, 54(5):3824–3851, 1996.
- [3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78(3):405–408, 1997.
- [4] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over $\text{GF}(4)$. *IEEE Trans. Information Theory*, 44(4):1369–1387, 1998.
- [5] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54(2):1098–1105, 1996.
- [6] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, 74(20):4091–4094, 1995.
- [7] P. Fire. A class of multiple-error-correcting binary codes for non-independent errors. Technical report, Sylvania Report RSL-E-2, Sylvania Reconnaissance Systems Laboratory, Mountain View, California, 1959.
- [8] D. Gottesman. A class of quantum error-correcting codes saturating the quantum hamming bound. *Phys. Rev. A*, 54(3):1862–1868, 1996.

- [9] M. Grassl, Th. Beth, and T. Pellizzari. Codes for the quantum erasure channel. *Phys. Rev. A*, 56(1):33–38, 1997.
- [10] E. Knill and R. Laflamme. A theory of quantum error-correcting codes. *Phys. Rev. A*, 55(2):900–911, 1997.
- [11] R. Laflamme, C. Miquel, J. Pablo Paz, and W. H. Zurek. Perfect quantum error correction code. *Phys. Rev. Lett.*, 77(1):198–201, 1996.
- [12] S. Lloyd. A potentially realizable quantum computer. *Science*, 261(1569–1571), 1993.
- [13] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error Correcting Codes*. North-Holland, New York, 1977.
- [14] C. M. Melas and E. Gorog. A note on extending certain codes to correct error bursts in longer messages. *IBM J. Res. Develop.*, 7:151–152, 1963.
- [15] G. M. Palma, K. A. Suominen, and A. K. Ekert. Quantum computers and dissipation. *Proc. of the Royal Soc. of London, Series A*, 452:567–584, 1996.
- [16] W. W. Peterson and Jr. E. J. Weldon. *Error-Correcting Codes*. MIT Press, 1972. 2nd ed.
- [17] E. Rains, April 1997. Private communication.
- [18] P. W. Shor. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A*, 52(4):2493–2496, 1995.
- [19] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77(5):793–797, 1996.
- [20] A. M. Steane. Multiple particle interference and quantum error correction. *Proc. of the Royal Soc. of London, Series A*, 452:2551–2577, 1996.